

PATENT APPLICATION  
ATTORNEY DOCKET NO. SUN-P4324-RSH

5

REPLACING AN EMAIL ATTACHMENT WITH  
10 AN ADDRESS SPECIFYING WHERE THE  
ATTACHMENT IS STORED

Inventors: Stephen R. Hanna, David C. Douglas, Yassir K. Elley,  
Radia J. Perlman, Sean J. Mullan and Anne H. Anderson

15

BACKGROUND

20 Field of the Invention

The present invention relates to computer systems and electronic mail.  
More specifically, the present invention relates to a method and an apparatus for  
replacing an attachment to an email message with a reference to a location where  
the attachment is stored.

25

Related Art

The advent of computer networks has led to an explosion in the  
development of applications that facilitate rapid dissemination of information. In  
particular, electronic mail is becoming the predominant method for  
30 communicating textual and other non-voice information. Using electronic mail, it

is just as easy to send a message to a recipient on another continent as it is to send a message to a recipient within the same building. Furthermore, an electronic mail message typically takes only a few minutes to arrive, instead of the days it takes for conventional mail to snake its way along roads and through airports.

5           Electronic mail messages commonly include attachments, which are typically files containing documents, or other types of data, that accompany the email message. However, using email attachments can give rise to a number of problems. (1) Attachments can create a burden for an email system. If an email message with a large attachment is sent to a large number of people (for example  
10 a baby picture sent to all 30,000 people in a company), the process of sending the attachment will take up a large amount of network bandwidth. Also, storing the attachment in a large number of mailboxes will take up a large amount of storage space. Furthermore, messages containing attachments may persist in mailboxes for a large period of time because people are not always diligent about reading and  
15 deleting email messages. (2) A user may accidentally forward an attachment. This is particularly a problem if the attachment contains confidential information that was not intended to be forwarded. (3) It is hard to control access to an attached file because anyone who receives a copy of the file can do anything they want with it. (4) Once a file is sent in an email, it is hard to subsequently update  
20 the file. It is possible to send a follow-on email, but this process is cumbersome. Furthermore, if the recipient makes changes to the file, it is hard to merge these changes back into the original file.

One method for overcoming these problems is to make the file accessible at a location on a server, and to send an address of the location, such as a uniform  
25 resource locator (URL), in the email message instead of the file. If this solution is combined with an access control/revision mechanism, it can potentially solve the above-listed problems.

However, this solution is cumbersome for a user who sends a file. Making a file available on a server requires a significant amount of effort to manually copy the file to the server, and to configure the server to make the file accessible over a communication channel. Furthermore, end users typically do not have permission to perform these operations, and establishing access/revision controls can be complicated.

What is needed is a method and an apparatus that automatically makes email attachments available on a server without requiring the attachments to be manually copied and configured on the server.

10

### SUMMARY

One embodiment of the present invention provides a system that replaces an attachment to an email message with a reference to a location where the attachment is stored. Upon receiving the email message, the system examines the email message to determine if the email message includes an attachment. If the email message includes the attachment, the system stores the attachment at a location on a communication network from which the attachment can be retrieved.

The system also modifies the email message by replacing the attachment with a reference specifying the location of the attachment, and sends the modified email message to a recipient of the email message.

In one embodiment of the present invention, the recipient receives the modified email message and uses the reference specifying the location of the attachment to retrieve the attachment across the communication network.

In one embodiment of the present invention, retrieving the attachment includes authenticating the recipient to a computer system upon which the attachment is stored.



## BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 illustrates computer systems coupled together by a network in accordance with an embodiment of the present invention.

FIG. 2 illustrates how an email message with an attachment travels  
5 between computer systems in accordance with an embodiment of the present invention.

FIG. 3 is a flow chart illustrating the process of replacing an email attachment with a reference to a location where the attachment is stored in accordance with an embodiment of the present invention.

10

## DETAILED DESCRIPTION

The following description is presented to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed  
15 embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features  
20 disclosed herein.

The data structures and code described in this detailed description are typically stored on a computer readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. This includes, but is not limited to, magnetic and optical storage devices such as disk  
25 drives, magnetic tape, CDs (compact discs) and DVDs (digital video discs), and computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated). For example, the

transmission medium may include a communications network, such as the Internet.

### **Computer System**

5           FIG. 1 illustrates computer systems 102, 108-109, 111 and 114-115 coupled together by network 106 in accordance with an embodiment of the present invention. Network 106 can include any type of wire or wireless communication channel capable of coupling together computer systems. This includes, but is not limited to, a local area network, a wide area network, or a  
10       combination of networks. In one embodiment of the present invention, network 106 includes the Internet. Network 106 can also include a communication pathway through a telephone line.

          The computer systems illustrated in FIG. 1 include sender 102, recipients 114-115, email servers 108-109, and file server 111. The computer system in  
15       FIG. 1 may optionally include firewall 104. Firewall 104 may be located in a separate computer system, or alternatively, may be integrated into sender 102. Note that computer systems 102, 108-109, 111, and 114-115 can generally include any type of computer system, including, but not limited to, a computer system based on a microprocessor, a mainframe computer, a digital signal processor, a  
20       personal organizer, a device controller, and a computational engine within an appliance.

          More specifically, sender 102 can include any computer system that can send an email message. Recipients 114-115 can include any computer system that can receive an email message. Email servers 108-109 can include any computer  
25       systems through which an email message travels between sender 102 and recipients 114-115. Note that an email message typically travels through one or more email servers in its path from sender to recipient.

Email server 108 includes distribution list exploder (DLE) 110. DLE 110 keeps track of a set of recipients specified in a distribution list. Upon receiving an email message sent to the distribution list, DLE 110 forwards the email message to the set of recipients.

5           File server 111 can include any system that can store an email attachment, and that can make the attachment available across a communication channel, such as network 106. In one embodiment of the present invention, file server 111 is implemented as a web server. Note that file server 111 may exist within another computer system, such as email server 108, or may exist in a stand-alone  
10       computer system.

          Firewall 104 can include any mechanism that protects sender 102 from communications across network 106. All communications between sender 102 and network 106 pass through firewall 104, which allows firewall 104 to screen these communications for security purposes.

15

#### **Path of an Email Message**

          FIG. 2 illustrates how an email message 202 with an attachment 204 travels between computer systems in accordance with an embodiment of the present invention. First, sender 102 sends email message 202 (including  
20       attachment 204) to email server 108. Note that email message 202 is addressed to recipient 114, but the email system automatically directs email message 202 through email server 108.

          Also note that attachment 204 can include any type of file or other data that can be attached to an email message. For example, attachment 204 can  
25       include a document, a graphical image or a data file.

          Email server 108 sends attachment 204 to file server 111 so that file server can make attachment 204 available over network 106 at an address specified by

URL 206. Email server 108 also forwards email message 202 along with URL 206 to email server 109. Email server 109 then sends email message 202 and URL 206 to recipient 114 (potentially through other email servers). Email server 108 can also send email message 202 and URL 206 directly to recipient 114 without passing through email server 109.

Upon receiving email message 202 and URL 206, recipient 114 uses URL 206 to send a request 208 for attachment 204 to file server 111. In response to request 208, file server 111 sends attachment 204 to recipient 114.

#### 10 **Process of Replacing an Attachment with a Reference**

FIG. 3 is a flow chart illustrating the process of replacing an email attachment with a reference to a location where the attachment is stored in accordance with an embodiment of the present invention. Note that this process can take place in a number of different locations, including within an email client application on sender 102, at email server 108, at email server 109, at firewall 104, at a gateway that changes the format of email message 202 (perhaps located within firewall 104), or at any other computer system that is capable of performing the process. Alternatively, the process can be split up between multiple computer systems.

Note that if the process takes place outside of sender 102 and recipient 114, the system can be implemented without modifying existing email applications on sender 102 and recipient 114.

The system starts by receiving an email message 202 (step 302). If the email message 202 does not include an attachment 204, then the system sends email message 202 to recipient 114 (step 305). Note that sending email message 202 to recipient 114 may include waiting for recipient 114 to retrieve email message 202 from an email server, such as email server 109.



If email message 202 includes attachment 204, the system stores attachment 204 to file server 111 (step 306). In one embodiment of the present invention, the system sets up access controls on file server 111 so that only authorized entities are able to view and/or modify attachment 204. A default set of access controls allows a sender of an email message to read from and write to the associated attachment, while recipients are only allowed to read from the attachment.

As a performance enhancement, the system may additionally merge references to files that have already been stored to avoid storing them twice. In this case, it may be desirable to use a different URL to refer to the same file, so that the file can be copied if one of the versions of the file is later updated.

In one embodiment of the present invention, the system requires administrative approval before making attachment 204 available on file server 111.

Next, the system modifies email message 202 by replacing attachment 204 with URL 206 (or any other reference for the location of attachment 204 on file server 111) (step 308). Note that if the replacement process is carried out on sender 102, then the system can easily ask the user if the user wants to replace the attachment with URL 206.

Carrying out the replacement process on sender 102 also allows the system to create a digital signature for email message 202 including URL 206. Otherwise, if email message 202 is modified after a digital signature is created for email message 202, then the modification process will invalidate the digital signature.

The modified email message 202, including URL 206, is then sent to all recipients, including recipient 114 (step 310). In one embodiment of the present invention, the last component in URL 206 matches the filename of the original

attachment 204 so that the attachment can be identified in case the body of email message 202 refers to the attachment 204 by name. In one embodiment of the present invention, preceding components in URL 206 are chosen to distinguish attachments with identical names.

5           A number of methods can be used to send email to recipients on a distribution list through a DLE, such as DLE 110. (1) The system can place all recipients on an access control list. (2) The system can put the alias for the distribution list on the access control list and can require recipients to prove membership in the alias (or some other related group). (3) The system can put the  
10       alias on the access control list, and can determine whether a recipient is on the alias when the recipient attempts to access the attachment.

          Upon receiving modified email message 202 including URL 206 (step 312), recipient 114 uses URL 206 to retrieve attachment 204 from file server 111 (step 314). This may involve allowing a user to explicitly request attachment 204  
15       by clicking on URL 206.

          In order to receive attachment 204, recipient 114 may have to be authenticated to file server 111. This can be accomplished using any of a number of authentication mechanisms, such as a password, a shared secret, public key cryptography and/or digital certificates. Attachment 204 may additionally be  
20       encrypted to provide additional security.

          One of the advantages of the above-described embodiment is that it can provide better proof of receipt of a file. Proof of receipt is rarely provided for email messages. By forcing recipient 114 to log onto file server 111 to receive attachment 204, proof of receipt can be obtained.

25           However, proving the exact contents of the attachment received is more difficult. In order to do so, one embodiment of the present invention delivers an encrypted version of attachment 204 to recipient 114. Recipient 114 must sign a

receipt (possibly including a hash of the encrypted attachment) in order to receive the decryption key.

At a later point in time, the system allows attachment 204 to be modified on file server 111 subject to the above-described access control rules (step 316).

5 Eventually, the system deletes attachment 204 from file server 111. This deletion process can take place in a number of different ways. It can take place automatically after an expiration of a time period. It can take place after sending a notification to recipients of the email message that the attachment will be deleted.

It can take place after receiving a notification that all recipients of the email  
10 message have retrieved the attachment. It can take place after receiving a notification that all recipients of the email message have deleted the email message. It can take place after receiving a command from a sender of the email message to delete the attachment (perhaps after some nagging). Alternatively, attachment 204 can be stored in a user's workspace so that the user will delete it  
15 during a normal cleanup operation. Note that it is often desirable to store attachment 204 to archival storage before deleting it from file server 111, so that it can be retrieved at a later time if necessary.

In one embodiment of the present invention, the system allows recipient  
20 114 to forward URL 206 to another recipient and to delegate its access privileges to the other recipient if sender 102 does not object.

In one embodiment of the present invention, sender 102 can update attachment 204 by sending a follow-up email message with an indication that attachment 204 should be replaced with a new version of attachment 204. Upon receiving this follow-up email message, the system performs the replacement.  
25 This can alternatively be accomplished through an explicit command entered through an email program.

